

Limits of the Kučera-Gács coding method*

George Barmpalias

Andrew Lewis-Pye

March 31, 2017

Abstract. Every real is computable from a Martin-Löf random real. This well known result in algorithmic randomness was proved by Kučera [Kuč85] and Gács [Gács86]. In this survey article we discuss various approaches to the problem of coding an arbitrary real into a Martin-Löf random real, and also describe new results concerning optimal methods of coding. We start with a simple presentation of the original methods of Kučera and Gács and then rigorously demonstrate their limitations in terms of the size of the redundancy in the codes that they produce. Armed with a deeper understanding of these methods, we then proceed to motivate and illustrate aspects of the new coding method that was recently introduced by Barmpalias and Lewis-Pye in [BLP16] and which achieves optimal logarithmic redundancy, an exponential improvement over the original redundancy bounds.

George Barmpalias

State Key Lab of Computer Science, Institute of Software, Chinese Academy of Sciences, Beijing, China. School of Mathematics, Statistics and Operations Research, Victoria University of Wellington, New Zealand.

E-mail: barmpalias@gmail.com. *Web:* <http://barmpalias.net>

Andrew Lewis-Pye

Department of Mathematics, Columbia House, London School of Economics, Houghton St., London, WC2A 2AE, United Kingdom.

E-mail: A.Lewis7@lse.ac.uk. *Web:* <http://aemlewis.co.uk>

*Barmpalias was supported by the 1000 Talents Program for Young Scholars from the Chinese Government, and the Chinese Academy of Sciences (CAS) President's International Fellowship Initiative No. 2010Y2GB03. Additional support was received by the CAS and the Institute of Software of the CAS. Partial support was also received from a Marsden grant of New Zealand and the China Basic Research Program (973) grant No. 2014CB340302.

1 Introduction

Information means structure and regularity, while randomness means the lack of structure and regularity. One can formalize and even quantify this intuition in the context of algorithmic randomness and Kolmogorov complexity, where the interplay between information and randomness has been a principal driving force for much of the research.

How much information can be coded into a random binary sequence? (1.0.1)

This question has various answers, depending on how it is formalized, but as we are going to see in the following discussion, for sufficiently strong randomness the answer is ‘not much’.

1.1 Finite information

In the case of a finite binary sequence (string) σ , let $K(\sigma)$ denote the prefix-free complexity of σ . Then σ is c -incompressible if $K(\sigma) \geq |\sigma| - c$. Here we view the underlying optimal universal prefix-free machine U as a *decompressor* or *decoder*, which takes a string/program τ and may output another string σ , in which case τ is regarded as a description of σ . Then $K(\sigma)$ is the length of the shortest description of σ and the random strings are the c -incompressible strings for some c , which is known as the *randomness deficiency*. It is well known that the shortest description of a string is random, i.e. there exists a constant c such that each shortest description is c -incompressible. In other words,

every string σ can be coded into a random string (its shortest description),
of length the Kolmogorov complexity of σ (1.1.1)

which may seem as a strong positive answer to Question (1.0.1), in the sense that every string σ can be coded into a random string. The following proposition, however, points in the opposite direction:

Proposition 1.1 (Folklore). *If U is an optimal universal prefix-free machine then there exists a constant c such that $U(\sigma) \uparrow$ for all strings σ such that $K(\sigma) \geq |\sigma| + c$.*¹

Viewing U as a universal decompressor, Proposition (1.1) says that a sufficiently random string cannot be decoded into anything, which means that in that sense it does not effectively code any information. According to this fact, Question (1.0.1) has a strong negative answer.

1.2 Bennett’s analogy for infinite information

The notions and issues discussed in the previous section have infinitary analogues which concern coding infinite binary sequences (*reals*) into random reals. For sufficiently strong (yet still moderate) notions of randomness for reals (such as the randomness corresponding to statistical tests or predictions that are definable in arithmetic with two quantifiers), the answer to Question (1.0.1) is *not much*; such random reals cannot solve the halting problem or even compute a complete extension of Peano Arithmetic.

¹The proof of this fact is based on the idea that each string in the domain of U is a prefix-free description of itself (modulo some fixed overhead). In other words, if $U(\sigma) \downarrow$ then σ can be used to describe itself, with respect to some prefix-free machine that is then simulated by U , producing a U -description of σ of length $|\sigma| + c$ for some constant c .

Charles Bennett (see [Ben88]) asked if Question (1.0.1) can have a strongly positive answer, just as in the finite case, for a standard notion of algorithmic randomness such as Martin-Löf randomness. Remarkably, Kučera [Kuč85] and Gács [Gács86] gave a positive answer to Bennett’s question.

Theorem 1.2 (Kučera-Gács theorem). *Every real is computable from a Martin-Löf random real.*

Bennett [Ben88] commented:

“This is the infinite analog of the far more obvious fact that every finite string is computable from an algorithmically random string (e.g. its minimal program).”

Here we argue that Bennett’s suggested analogy between (1.1.1) and Theorem 1.2 is not precise, in the sense that it misses the quantitative aspect of (1.1.1) – namely that the random code can be chosen short (of length the complexity of the string). It is much easier to code σ into a random string which is much longer than σ , than code it into a random string of length at most $|\sigma|$. The analogue of ‘length of code’ for infinite codes, is the *use-function* in a purported Turing reduction underlying the computation of a real X from a random real Y . The use function for the reduction is a function f such that for each n , the first n bits of X can be uniformly computed from the first $f(n)$ bits of Y .

1.3 A quantitative version of the Kučera-Gács theorem?

The more precise version of Bennett’s suggested analogy that we have just discussed can be summarized in Table 1, where σ^* denotes the shortest program for σ .² So what is the analogue of the code length in the Kučera-Gács theorem? If we code a real X into a Martin-Löf random real Y , how many bits of Y do we need in order to compute the first n bits of X ? This question has been discussed in the literature (see below) but, until recently, only very incomplete answers were known. Kučera [Kuč85] did not provide tight calculations and various textbook presentations of the theorem (e.g. Nies [Nie09, Section 3.3]) estimate the use-function in this reduction of X to a Martin-Löf random Y to be of the order n^2 . In fact, the actual bound that can be obtained by Kučera’s method is $n \log n$. Gács used a more elaborate argument and obtained the upper bound $n + \sqrt{n} \cdot \log n$, which is $n + o(n)$, and the same bound was also obtained later by Merkle and Mihailović [MM04] who used an argument in terms of supermartingales.

1.4 Coding into random reals, since Kučera and Gács

The Kučera-Gács coding method has been combined with various arguments in order to produce Martin-Löf random reals with specific computational properties. The first application already appeared in [Kuč89], where a high incomplete Martin-Löf random real computable from the halting problem was constructed. Downey and Miller [DM06] and later Barmpalias, Downey and Ng [BDN11] presented a variety of different versions of this method, which allow some control over the degree of the random real which is coded into. Doty [Dot06] revisited the Kučera-Gács theorem from the viewpoint of constructive dimension. He characterized the asymptotics of the redundancy in computations of an infinite sequence X from a random oracle in terms of the constructive dimension of X . We should also mention that this is not the only method for coding into members of a positive measure Π_1^0 class (or into the class

²If there are several shortest strings τ such that $U(\tau) = \sigma$ then σ^* denotes the one that converges the fastest.

<i>Notion</i>	<i>Finite</i>	<i>Infinite</i>
Source	σ	X
Code	σ^*	Y
Code-length	$ \sigma^* $	$n \mapsto f(n)$
Optimal code	$K(\sigma)$	$?$

Table 1: Quantitative analogy between finite and infinite codes; here $n \mapsto f(n)$ refers to an ‘optimal’ non-decreasing upper bound on the use-function in the computation of X from Y .

of Martin-Löf random reals). Barmpalias, Lewis-Pye and Ng [BLN10] used a different method in order to show that every degree that computes a complete extension of Peano Arithmetic is the supremum of two Martin-Löf random degrees.

It is fair to say that all of these methods rely heavily on the density of reals inside a nonempty Π_1^0 class that consists entirely of Martin-Löf reals. This is also true of more recent works such as Bienvenu, Greenberg, Kučera, Nies and Turetsky [BGK⁺15], Day and Miller [DM15] and Miyabe, Nies and Zhang [MNZ15]. Khan [Kha15] explicitly studies the properties of density inside Π_1^0 classes, not necessarily consisting entirely of Martin-Löf random reals. Much of this work is concerned with lower bounds on the density that a Martin-Löf real has inside every Π_1^0 class that contains it. In our analysis of the Kučera-Gács theorem we isolate the role of density in the argument and show that, in a sense, tighter oracle-use in computations from Martin-Löf random oracles is only possible through methods that do not rely on such density requirements.

2 Coding into an effectively closed set subject to density requirements

The arguments of Kučera and Gács both provide a method for coding an arbitrary real X into a member of an effectively closed set P (a Π_1^0 class), and rely on certain density requirements for the set of reals \mathcal{P} . The connection to Theorem 1.2 is that the class of Martin-Löf random reals is the effective union of countably many Π_1^0 classes of positive measure. The only difference in the two methods is that Kučera codes X one-bit-at-a-time (with each bit of X coded into a specified segment of Y) while Gács codes X block-by-block into Y , with respect to a specified segmentation of X .

2.1 Overview of the Kučera-Gács argument

In general, we can code m_i many bits of X at the i th coding step, using a block in Y of length ℓ_i , as Table 2 indicates. We leave the parameters $(m_i), (\ell_i)$ unspecified for now, while in the following it will become clear what the growth of this sequence needs to be in order for the argument to work. Note that the bit-by-bit version of the coding is the special case where $m_i = 1$ for all i . The basic form of the coding process (which we shall elaborate on later) can be outlined as follows.

m_i	Length of the i th block of X
ℓ_i	Length of the i th block of Y
M_n	Number of bits of X coded after n -many coding steps: $M_n := \sum_{i < n} m_i$
L_n	Length of Y used in the computation of $X \upharpoonright_{M_n}$: $L_n := \sum_{i < n} \ell_i$

Table 2: Parameters of the Kučera-Gács coding of X into Y

- (1) Start with a Π_1^0 class $\mathcal{P} \neq \emptyset$ which only contains (Martin-Löf) randoms.
- (2) Choose the *length m_i of the block* coded at step i .
- (3) Choose the length $\ell_i = m_i + g(i)$ used for coding the i th block.
- (4) The *oracle-use* for the first $M_n = \sum_{i < n} m_i$ bits is $L_n = \sum_{i < n} \ell_i$.
- (5) Form a subclass \mathcal{P}^* of \mathcal{P} with the property that for all but finitely many n and for each $X \in \mathcal{P}^*$, there are at least 2^{m_n} extensions of $X \upharpoonright_{L_n}$ of length L_{n+1} which have infinite extensions in \mathcal{P}^* .
- (6) Argue that $\mathcal{P}^* \neq \emptyset$ (due to the growth of (ℓ_i) , relative to (m_i)).

A crucial fact here is that if \mathcal{P} is a Π_1^0 class then \mathcal{P}^* is also a Π_1^0 class. In Section 2.2 we turn this outline into a modular proof, which makes the required properties of the parameters $(m_i), (\ell_i)$ transparent. We will show that apart from the computability of $(m_i), (\ell_i)$, the following facts characterize the necessary and sufficient constraints on the two sequences for the coding to work.

- (i) If $\sum_i 2^{m_i - \ell_i} < \infty$ then there exists a Π_1^0 class of positive measure that consists entirely of Martin-Löf random reals such that $\mathcal{P}^* \neq \emptyset$;
- (ii) If $\sum_i 2^{m_i - \ell_i} = \infty$ and \mathcal{P} is a Π_1^0 class such that $\mathcal{P}^* \neq \emptyset$ then \mathcal{P} contains a real which is not Martin-Löf random.

2.2 The general Kučera-Gács argument

We give a modular argument in terms of Π_1^0 classes, showing that every real is computable from a Martin-Löf random real, and consisting of a few simple lemmas. We use Martin-Löf's paradigm of algorithmic randomness, much like in the original argument of Kučera and Gács.³ In the next definition, recall that for finite σ , $[\sigma]$ is the set of all infinite extensions of σ .

Definition 2.1 (Extension property). *Given a Π_1^0 class P and sequences $(m_i), (\ell_i)$ of positive integers, let $M_n := \sum_{i < n} m_i$, $L_n := \sum_{i < n} \ell_i$ and say that P has the extension property with respect to $(m_i), (\ell_i)$ if for each i , every string σ of length L_i with $[\sigma] \cap P \neq \emptyset$ has at least 2^{m_i} extensions τ of length L_{i+1} such that $P \cap [\tau] \neq \emptyset$.*

³However our presentation has been significantly assisted by Merkle and Mihailović [MM04], who phrased the argument in terms of martingales.

$\ell_i - m_i$	Overhead at the i th coding step
$\sum_{i < n} (\ell_i - m_i)$	Accumulated overhead after n coding steps
$\sum_i 2^{m_i - \ell_i} < \infty$	Necessary and sufficient condition for successful coding

Table 3: Overheads in the Kučera-Gács coding of X into Y

The first lemma says that subject to certain density conditions on a Π_1^0 class P , every real is computable from a member of P .

Lemma 2.2 (General block coding). *Suppose that P is a Π_1^0 class, and (m_i) , (ℓ_i) are computable sequences of positive integers. If P has the extension property with respect to (m_i) , (ℓ_i) , then every sequence is computable from a real in P with use L_{s+1} for bits in $[M_s, M_{s+1})$.*

Proof. For any string σ of length L_i consider the variables $w_0(\sigma)[s], \dots, w_{2^{m_i}-1}(\sigma)[s]$ for strings, which are defined dynamically according to the approximation (P_s) to P as follows. At stage 0 let $w_j(\sigma)[0] \uparrow$ for all $j < 2^{m_i}$. At stage $s + 1$ find the least $t < 2^{m_i}$ such that one of the following holds:

- (a) $w_t(\sigma)[s] \uparrow$;
- (b) $w_t(\sigma)[s] \downarrow$ and $[w_t(\sigma)[s]] \cap P_{s+1} = \emptyset$.

In case (a) look for the lexicographically least ℓ_i -bit extension τ of σ such that $[\tau] \cap P_{s+1} \neq \emptyset$ and $w_j(\sigma)[s] \neq \tau$ for all $j < 2^{m_i}$. If no such exists, terminate the process (hence let $w_j(\sigma)[n] \simeq w_j(\sigma)[s]$ for all $j < 2^{m_i}$ and all $n > s$). Otherwise define $w_t(\sigma)[s + 1] = \tau$ and go to the next stage. In case (b) let $w_t(\sigma)[s + 1] \uparrow$ and go to the next stage.

By the hypothesis of the lemma, for every i and every string σ of length L_i such that $[\sigma] \cap P \neq \emptyset$, the words $w_j(\sigma)[s]$, $j < 2^{m_i}$ reach limits $w_j(\sigma)$ after finitely many stages, such that:

- $j \neq k \Rightarrow w_j(\sigma) \neq w_k(\sigma)$ for all $j, k < 2^{m_i}$;
- $[w_j(\sigma)] \cap P \neq \emptyset$.

Consider the Turing functional Φ which, given oracle Y , works inductively as follows. Suppose that $\Phi(Y \upharpoonright_{L_i}) \upharpoonright_{M_i}$ has been calculated. The functional then searches for the least pair (j, s) (under a fixed effective ordering of all pairs, of order type ω) such that $j < 2^{m_i}$, $w_j(Y \upharpoonright_{L_i})[s] \downarrow$ and is a prefix of Y . For τ which is the j th string of length m_i (under the lexicographical ordering) the functional then defines $\Phi(Y \upharpoonright_{L_i+\ell_i}) = \Phi(Y \upharpoonright_{L_i}) * \tau$. By construction Φ is consistent, and if $\Phi(Y \upharpoonright_{L_i})$ is defined it has length M_i . Finally we show that Φ is onto the Cantor space. Given X we can inductively construct Y such that $\Phi(Y) = X$. Suppose that we have constructed $Y \upharpoonright_{L_i}$ such that $\Phi(Y \upharpoonright_{L_i}) = X \upharpoonright_{M_i}$ and $Y \upharpoonright_{L_i}$ is extendible in P . Let σ be the unique string of length m_i such that $X \upharpoonright_{M_i} * \sigma$ is a prefix of X . Then $w_j(Y \upharpoonright_{L_i})$ is defined for all $j < 2^{m_i}$ and takes distinct values for different j . Let t be the index of σ in the lexicographical ordering of strings of length m_i . Then let $Y \upharpoonright_{L_{i+1}} = w_t(Y \upharpoonright_{L_i})$. Clearly $Y \upharpoonright_{L_{i+1}}$ is extendible in P and moreover $\Phi(Y \upharpoonright_{L_{i+1}}) = X \upharpoonright_{M_{i+1}}$. This completes the induction step in the construction of Y and shows that $\Phi(Y) = X$. \square

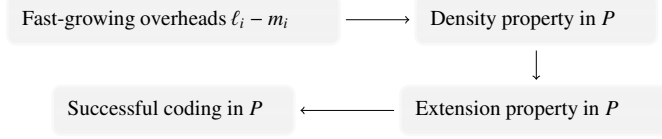


Figure 4: Diagrammatic representation of the Kučera-Gács coding argument.

Recall that for σ of length n , the P -density of σ is defined to be $2^n \cdot \mu([\sigma] \cap P)$, where μ denotes Lebesgue measure on Cantor space.

Definition 2.3 (Density property). *Given P , (m_i) , (ℓ_i) as in Definition 2.1 we say that P has the density property with respect to (m_i) , (ℓ_i) if for each n , every string of length L_n with $[\sigma] \cap P \neq \emptyset$ has P -density at least $2^{m_n - \ell_n}$.*

Lemma 2.4 (Density and extensions). *Given P , (m_i) , (ℓ_i) as in Definition 2.1, if P has the density property with respect to (m_i) , (ℓ_i) then it also has the extension property with respect to (m_i) , (ℓ_i) .*

Proof. This follows from the general fact that if the P -density of σ is at least 2^{-t} for some t , then given any m , there are at least 2^m extensions τ of σ of length $|\sigma| + t + m$ such that $[\tau] \cap P \neq \emptyset$. In order to prove the latter fact, suppose for a contradiction that it is not true. Then the P -density of σ would be at most $(2^m - 1) \cdot 2^{-m-t} = 2^{-t} - 2^{-m-t} < 2^{-t}$ which contradicts the hypothesis. \square

Lemma 2.5 (Lower bounds on the density). *Let P be a Π_1^0 class and let (m_i) , (ℓ_i) be computable sequences of positive integers such that $\sum_i 2^{m_i - \ell_i} < \mu(P)$. Then there exists a Π_1^0 class $P^* \subseteq P$ which has the extension property with respect to (m_i) , (ℓ_i) .*

Proof. We construct a Σ_1^0 class Q in stages and let (P_s) be a Π_1^0 approximation to P , where each P_s is a clopen set. A string σ is *active* at stage $s + 1$ if it is of length L_n for some n and $[\sigma] \cap (P_s - Q_s) \neq \emptyset$. Moreover σ of length L_n *requires attention* at stage $s + 1$ if it is active at this stage and the $(P_s - Q_s)$ -density of σ is at most $2^{m_n - \ell_n}$. At stage $s + 1$, we pick the least string of length $< s$ which requires attention (if such exists) and enumerate $[\sigma] \cap (P_s - Q_s)$ into Q . If this enumeration occurred, we say that the construction acted on string σ at stage $s + 1$. This concludes the construction.

First we establish an upper bound on the measure of $Q = \cup_s Q_s$. Clearly the construction can act on a string at most once. The measure that is added to Q at stage $s + 1$ if the construction acts on σ of length L_n at this stage, is at most $2^{-L_n + m_n - \ell_n}$. Therefore the total measure enumerated into Q throughout the construction is bounded above by:

$$\sum_n \sum_{\sigma \in 2^{L_n}} 2^{-L_n + m_n - \ell_n} = \sum_n 2^{L_n} \cdot 2^{-L_n + m_n - \ell_n} = \sum_n 2^{m_n - \ell_n} < \mu(P).$$

It follows that $P^* := P - Q$ is a nonempty Π_1^0 class, and by the construction we have that for every n and every string σ of length L_n , if $[\sigma] \cap P^* \neq \emptyset$ then the P^* -density of σ is at least $2^{m_n - \ell_n}$. By Lemma 2.4 this means that every P^* -extendible string of length L_n for some n has at least 2^{m_n} many P^* -extendible extensions of length $L_n + m_n - (m_n - \ell_n) = L_{n+1}$. Hence P^* has the extension property with respect to (m_i) , (ℓ_i) . \square

Corollary 2.6 (General block coding). *Suppose that P is a Π_1^0 class, and $(m_i), (\ell_i)$ are computable sequences of positive integers. If $\sum_i 2^{m_i - \ell_i} < \mu(P)$ then every sequence is computable from a real in P with use L_{s+1} for bits in $[M_s, M_{s+1})$.*

Proof. By Lemma 2.5 we can consider a Π_1^0 class $P^* \subseteq P$ which has the extension property with respect to $(m_i), (\ell_i)$. The statement then follows by Lemma 2.2 and the fact that $P^* \subseteq P$. \square

Note that, while Corollary 2.6 seems to require (a) $\sum_i 2^{m_i - \ell_i} < \mu(P)$, if P is of positive measure then the condition (b) $\sum_i 2^{m_i - \ell_i} < \infty$ suffices to ensure that $\sum_{i \geq d} 2^{m_i - \ell_i} < \mu(P)$ for some d – meaning that (b) is sufficient to give the existence of the required functional (albeit with some added non-uniformity required in specifying the index of the reduction).

2.3 The oracle-use in the general Kučera-Gács coding argument

Recall that if X can be computed from Y with the use function on argument n bounded by $n + g(n)$, then we say that X can be computed from Y with *redundancy* $g(n)$. Note that in the following corollary we do not need to require that h, h_r are computable.

Corollary 2.7. *Suppose $(m_i), (\ell_i)$ are computable sequences of positive integers with $\sum_i 2^{m_i - \ell_i} < 1$ and suppose h, h_r are nondecreasing functions such that:*

$$\sum_{i \leq s} \ell_i \leq h \left(1 + \sum_{i < s} m_i \right) \quad \text{and} \quad m_s + \sum_{i \leq s} (\ell_i - m_i) \leq h_r \left(\sum_{i < s} m_i \right).$$

Then if P is a Π_1^0 class of positive measure, any sequence is computable from a real in P with oracle-use h and redundancy h_r .

Proof. The first claim follows directly from Corollary 2.6 and for the second, recall that in the same corollary, for each s and each $n \in [M_s, M_{s+1})$, the length of the initial segment of Y that is used for the computation of $X \upharpoonright_n$ is at most

$$L_{s+1} = M_s + m_s + \sum_{i \leq s} (\ell_i - m_i) \leq n + m_s + \sum_{i \leq s} (\ell_i - m_i) \leq n + h_r(M_s) \leq n + h_r(n)$$

where the second inequality was obtained from the main property assumed for h_r , and the last inequality follows from the monotonicity of h_r . \square

Without yet specifying the sequences $(m_i), (\ell_i)$, the condition $\sum_i 2^{m_i - \ell_i} < 1$ means that a near-optimal choice for the sequence $(\ell_i - m_i)$ is $\lceil 2 \log(i + 2) \rceil$. This means that $\sum_i (\ell_i - m_i)$ will be of the order $\log(n!)$ or $n \log n$. We may now consider an appropriate choice for the sequence (m_i) , which roughly minimizes the redundancy established in Corollary 2.7. For Kučera's coding we have $m_i = 1$ for all i which means that the redundancy in this type of bit-by-bit coding is $n \log n$ (modulo a constant). Gács chose the sequence $m_i = i + 1$, and the reader may verify that this growth-rate of the blocks of the coded

stream gives a near-optimal redundancy in Corollary 2.7.⁴ In this case the function $h_r(n) = \sqrt{n} \cdot \log n$ satisfies the second displayed inequality of Corollary 2.7 (for almost all n), since $n + 1 + n \log n \leq \sqrt{(n+1)n/2} \cdot \log((n+1)n/2)$ for almost n . Hence every real is computable from a Martin-Löf random real with this redundancy, much like Gács had observed.

We can now intuitively understand how the redundancy upper bounds $n \log n$ and $\sqrt{n} \cdot \log n$, of Kučera and Gács respectively, are produced. The argument of Section 2.2 describes a coding process where in n coding steps we code M_n many bits of X into L_n many bits of Y . The parameter $g(i) := \ell_i - m_i$ can be seen as an *overhead* of the i th coding step, i.e. the number of additional bits we use in Y in order to code the next m_i bits of X . Moreover, Corollary 2.7 says that these overheads are accumulated along the coding steps and push the redundancy of the computation to become larger over time. In particular, the number $\sum_{i < n} g(i)$ is the redundancy (total overhead accumulated) corresponding to n coding steps. Due to the condition $\sum_i 2^{-g(i)} < 1$ in Corollary 2.7 a representative choice for g is $2 \log(n+1)$, which means that $\sum_{i < n} g(i)$ needs to be of the order $\log(n!)$ or (by Stirling's formula) $n \log n$.

In the case of Kučera's argument, n bits of X are coded in n coding steps, so the redundancy for the computation of n bits of X from Y following Kučera's argument is of the order $n \log n$. If we are free to choose (m_i) , note that a fast-growing choice will make the accumulated overhead smaller (since the coding steps for any initial segment of X become less) but a different type of overhead, namely the parameter m_s in the second inequality of Corollary 2.7, pushes the redundancy higher. Gács' choice of $m_i = i + 1$ means that in n coding steps there are $\sum_{i \leq n} m_i \approx n^2$ many bits of X coded into Y . Hence the coding of $X \upharpoonright_n$ requires roughly \sqrt{n} coding steps, which accumulate a total of $\sqrt{n} \cdot \log \sqrt{n} \approx \sqrt{n} \cdot \log n$ in overheads according to the previous discussion. For this reason, Gács' redundancy is of the order $\sqrt{n} \cdot \log n$. We may observe that in Gács' coding, the length of the next coding block m_{n+1} is both:

- (a) the number of coding steps performed so far;
- (b) roughly equal to the accumulated overhead from the coding steps performed so far.

2.4 Some limits of the Kučera-Gács method

In this section we will frequently identify a set of finite strings V with the Σ_1^0 class specified by V , i.e. the set of infinite sequences extending elements of V . In the following proof we use the notation $\mu_\sigma(C)$ for a string σ and a set of reals C , which is the measure of C relative to $[\sigma]$. More precisely $\mu_\sigma(C) = \mu(C \cup [\sigma]) \cdot 2^{|\sigma|}$.

Lemma 2.8. *Let P be a Π_1^0 class, g a computable function taking positive values, such that $\sum_i 2^{-g(i)} = \infty$. Let (n_i) be a computable sequence such that $n_{i+1} > n_i + g(i)$ for all i . If*

$$(U_i) \text{ is a uniformly c.e. sequence with } U_i \subseteq 2^i \text{ and } \mu(P \cap U_i) < 2^{-i} \text{ for all } i$$

then every Martin-Löf random real $X \in \cap_i (P \cap U_i)$ has a prefix in some U_{n_i} with P -density at most $2^{-g(i)}$.

⁴For example the choices $m_i = (i+1)^2$ or $m_i = \sqrt{i+1}$ produce redundancy considerably above Gács' $\sqrt{n} \cdot \log n$ upper bound.

Proof. We define a uniform sequence (V_i) of Σ_1^0 classes such that $V_t \supseteq V_{t+1}$ for all t , inductively as follows. Let V_0 (as a set of finite strings) consist of all the strings of length n_0 . Assuming that V_t has been defined, for each $\sigma \in V_t$ define

$$V_{t+1} \cap [\sigma] = (U_{n_{t+1}} \cap [\sigma])^{[\leq 2^{-|\sigma|} \cdot (1 - 2^{-g(t)-1})]},$$

where for any real r and any Σ_1^0 class C with an underlying computable enumeration $C[s]$ the expression $C^{[\leq r]}$ denotes the class $C[s_*]$ where s_* is the largest stage s such that $\mu(C[s]) \leq r$ if such a stage exists, and $s_* = \infty$ otherwise (in which case we let $C[\infty] = C$). Clearly for each t the set V_t consists of strings of length n_t . Then for each t we have $\mu(V_{t+1}) \leq (1 - 2^{-g(t)-1}) \cdot \mu(V_t)$ so

$$\mu(V_{t+1}) \leq \prod_{i=0}^t (1 - 2^{-g(i)-1}).$$

By hypothesis, $\sum_i 2^{-g(i)} = \infty$ so $\prod_{i=0}^{\infty} (1 - 2^{-g(i)-1}) = 0$. Since g is computable, there exists a computable increasing sequence (k_i) such that $\prod_{i=0}^{k_t} (1 - 2^{-g(i)-1}) < 2^{-t}$ for all $t > 0$. Hence (V_{k_i}) is a Martin-Löf test. Now let X be a Martin-Löf random real with $X \in \cap_i (P \cap U_i)$, as in the statement of the lemma. Since X is Martin-Löf random, $X \notin \cap_i V_{k_i} = \cap_i V_i$ and there exists a maximum t such X has a prefix σ in V_t . By the maximality of t we have $X \notin V_{t+1}$ and since $X \in U_{n_{t+1}}$ we must have $\mu_\sigma(U_{n_{t+1}}) > 1 - 2^{-g(t)-1}$, because otherwise a prefix of X would enter V_{t+1} . Also $\mu_\sigma(P \cap U_{n_{t+1}}) \leq 2^{|\sigma|} \cdot \mu(P \cap U_{n_{t+1}}) \leq 2^{|\sigma| - n_{t+1}}$. Since $\sigma \in V_t$, the length of σ is n_t . Since $n_{t+1} > n_t + g(t)$ we have $\mu_\sigma(P \cap U_{n_{t+1}}) \leq 2^{-g(t)-1}$. From the fact that

$$\mu_\sigma(P) + \mu_\sigma(U_{n_{t+1}}) - \mu_\sigma(P \cap U_{n_{t+1}}) \leq 1$$

we can deduce that $\mu_\sigma(P) \leq 2^{-g(t)}$. Since σ is a prefix of X of length n_t , this concludes the proof. \square

Corollary 2.9. Suppose that $(m_i), (\ell_i)$ are computable sequences of positive integers with $\sum_i 2^{m_i - \ell_i} = \infty$. Then every Π_1^0 class consisting entirely of Martin-Löf random reals, which has the density property with respect to $(m_i), (\ell_i)$, is empty.

Proof. We apply Lemma 2.8 with $n_k = L_k = \sum_{i < k} \ell_i$ and $g(i) = \ell_i - m_i$. First note that $n_{k+1} = n_k + \ell_k > n_k + g(k)$ because $g(k) < \ell_k$, so the hypothesis of Lemma 2.8 for (n_i) holds. Second, for each i let σ_i^* be the leftmost P -extendible string of length i and let U_i consist of σ_i^* as well as the strings of length i which are lexicographically to the left of σ_i^* . Then (U_i) is uniformly c.e. and $\mu(P \cap U_i) = \mu(P \cap [\sigma_i^*]) \leq 2^{-i}$ for all i . Now suppose that P is non-empty and consider the leftmost path X through P . By our assumptions regarding P , the real X is Martin-Löf random, so by Lemma 2.8 there exists some k such that the P -density of $X \upharpoonright_{L_k}$ is less than $2^{m_k - \ell_k}$. This means that there is a P -extendible string of length L_k with P -density below $2^{m_k - \ell_k}$, so P does not have the density property with respect to $(m_i), (\ell_i)$. \square

Corollary 2.10 (Lower bounds on the density inside a Π_1^0 class of random reals). Let P be a nonempty Π_1^0 class consisting entirely of Martin-Löf random reals, let g be a computable function, and let (L_i) be an increasing sequence of positive integers such that $L_{t+1} > L_t + g(t)$ for all t . Then the following are equivalent:

- (a) For every i the P -density of any P -extendible string of length L_i is $\Omega(2^{-g(i)})$
- (b) $\sum_i 2^{-g(i)} < \infty$

where the asymptotic notation $\Omega(2^{-g(i)})$ means $\geq 2^{-g(i)-c}$ for some constant c .

3 Coding into randoms without density assumptions

In [BLP16] a new coding method was introduced which allows for coding every real into a Martin-Löf random real with optimal, logarithmic redundancy. We call this method *density-free coding* as it does not rely on density assumptions inside Π_1^0 classes, which is also the reason why it gives an exponentially better redundancy upper bound.

Lemma 3.1 (Density-free coding, from [BLP16]). *Let (u_i) be a nondecreasing computable sequence and let \mathcal{P} be a Π_1^0 class. If $\sum_i 2^{i-u_i} < \mu(\mathcal{P})$ then every binary stream is uniformly computable from some member of \mathcal{P} with oracle-use (u_i) .*

Note that by letting P be a Π_1^0 class of Martin-Löf random reals of sufficiently large measure, Lemma 3.1 shows that every real is computable from a Martin-Löf random real with use $n + 2 \log n$, i.e. with logarithmic redundancy. On the other hand in [BLPT16] it was shown that this is optimal, in the sense that if $\sum_i 2^{i-u_i} = \infty$ then there is a real which is not computable from any Martin-Löf random real with use $n \mapsto u_n$. In particular, given a real ϵ , redundancy $\epsilon \cdot \log n$ in a computation from a random oracle is possible for every real if and only if $\epsilon > 1$.

We shall not give a proof of Lemma 3.1. Instead, we will discuss some aspects of this more general coding method, which contrasts the more restricted Kučera-Gács coding whose limitations we have already explored.

3.1 Coding as a labelling task

Coding every real into a path through a tree \mathcal{T} in the Cantor space involves constructing a Turing functional Φ which is onto the Cantor space, even when it is restricted to \mathcal{T} . In fact, this is normally done in such a way that there is a subtree \mathcal{T}^* of \mathcal{T} such that Φ is a bijection between $[\mathcal{T}^*]$ and 2^ω . In this case we refer to \mathcal{T}^* as the *code-tree*. Suppose we fix \mathcal{T} and consider constructing a functional for which the use u_n on argument n does not depend upon the oracle. Then the functional Φ can be constructed as a partial computable ‘labelling’ of the finite branches of \mathcal{T} . If the label x_σ is placed on τ , this means that Φ outputs σ when τ is the oracle. If we also suppose that the use function is strictly increasing, then the labelling might be assumed to satisfy the following conditions:

- (1) only strings of lengths $u_i, i \in \mathbb{N}$ of \mathcal{T} can have a label;
- (2) the labels placed on strings of length u_i of \mathcal{T} are of the type x_σ where $|\sigma| = i$;
- (3) if label x_σ exists in \mathcal{T} then all labels $x_\rho, \rho \in 2^{\leq |\sigma|}$ exist in \mathcal{T} ;
- (4) each string in \mathcal{T} can have at most one label;
- (5) if ρ of length u_k in \mathcal{T} has label x_σ then for each $i < k, \rho \upharpoonright_{u_i}$ has label $x_{\sigma \upharpoonright_i}$.

The reader may take a minute to view the Kučera coding as detailed in Section 2.2 as a labelling satisfying the properties (1)-(5) above. It is clear that:

The code-tree \mathcal{T}^* in the Kučera coding is isomorphic to the full binary tree.

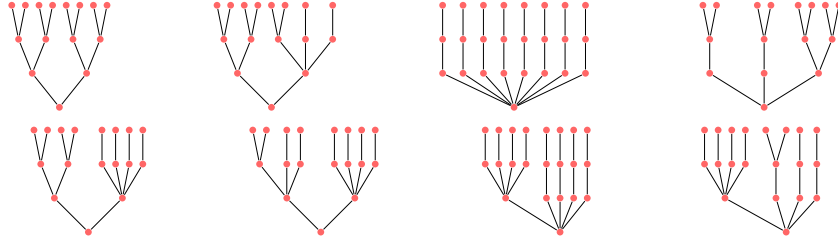


Figure 5: Some fully labellable (u_i) -trees of height 3.

The new coding behind Lemma 3.1 is also a labelling process, but in this case the code-tree can be much more complex.

3.2 Fully labelable trees

If (u_i) is an increasing sequence of positive integers, a (u_i) -tree T is a subset of $\{\lambda\} \cup (\cup_i 2^{u_i})$ which contains the empty string and is downward closed, in the sense that for each $\sigma \in 2^{u_{i+1}} \cap T$, the string $\sigma \upharpoonright_{u_i}$ belongs to T . The elements of a (u_i) -tree T are called nodes and the t -level of T consists of the nodes of T of length u_t . The full binary tree of height k is $2^{\leq k}$ ordered by the prefix relation. Note that a (u_i) -tree is a tree, in the sense that it is a partially ordered set (with respect to the prefix relation) in which the predecessors of each member are linearly ordered. Hence given any $k \in \mathbb{N}$, we may talk about a (u_i) -tree being isomorphic to the full binary tree of height k . When we talk about two trees being isomorphic, it is in this sense that we shall mean it – as partially ordered sets. A labelling of a (u_i) -tree is a partial map from the nodes of the tree to the set of labels $\{x_\sigma \mid \sigma \in 2^{<\omega}\}$ which satisfies properties (1)-(5) of the previous section. A full labelling of a (u_i) -tree is a labelling $\{x_\sigma \mid \sigma \in 2^{<\omega}\}$ with the property that for every σ there exists a node on the (u_i) -tree which has label x_σ .

A (u_i) -tree is called *fully labelable* if there exists a full labelling of it. Figure 5 illustrates some examples of fully labelable trees of height 3. Note that here the nodes are binary strings (hence nodes of the full binary tree) but since they are nodes of a (u_i) -tree, they can have more than two branches. Clearly, if $T_0 \subseteq T_1$ are (u_i) -trees and T_0 is fully labelable, then T_1 is also fully labelable. These definitions can be easily adapted to finite (u_i) -trees (where the height is the length of its longest leaf). Figure 5 shows some examples of fully labelable finite (u_i) -trees, while Figure 6 shows some examples of finite (u_i) -trees which are not fully labelable.

Clearly any (u_i) -tree which is isomorphic to the full binary tree, is fully labelable. The success of the Kučera coding was based on this fact, along with the fact that a Π_1^0 class of sufficient measure contains such a canonical tree (subject to the growth of (u_i)). A similar remark can be made about the slightly more general Gács coding. We have already demonstrated that the density property that guarantees the extension property cannot be expected to hold if the growth of (u_i) is significantly less than $n + \sqrt{n} \cdot \log n$. Hence more efficient coding methods, such as the one behind Lemma 3.1, need to rely on a wider class of labelable trees.

Given two trees T_0, T_1 (thought of as partially ordered sets), we say that T_0 is *splice-reducible* to T_1

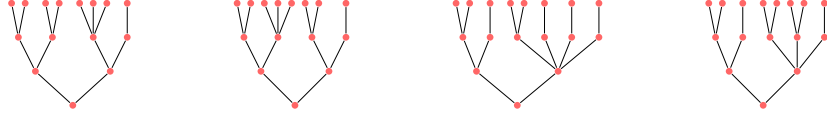


Figure 6: Some (u_i) -trees of length 3 which are not fully labelable.

if we can obtain T_1 from T_0 via a series of operations on the nodes of T_0 , each consisting of splicing two sibling nodes into one – i.e. the two sibling nodes u_0 and u_1 are replaced by a single node u , for which the set of elements $> u$ is isomorphic to the set of nodes strictly greater than u_0 union the set of nodes strictly greater than u_1 . The following result points to a concrete difference between Kučera coding and the general coding from [BLP16]: in Kučera coding the code-tree is an isomorphic copy of the full binary tree, while in [BLP16] the code-tree is only splice-reducible to an isomorphic copy of the full binary tree.⁵

Theorem 3.2. *Given a (u_i) -tree T , the following are equivalent:*

- (a) *T is a fully labelable (u_i) -tree;*
- (b) *T is splice-reducible to an isomorphic copy of the full binary tree.*

Proof. Suppose that T is fully labelable. We describe how to produce the full binary tree by a repeated application of the splice operation between siblings of T . Fix a full labelling of T and obtain the minimal fully labeled tree T' from T by splicing the unlabelled nodes of T onto labelled ones. Now all nodes of T' are labelled. Then gradually, starting from the first level and moving toward the last level of T' , splice siblings with identical labels. Inductively, by the properties of the assumed labelling, the resulting (u_i) -tree is isomorphic to the full binary tree.

Conversely, assume that T is splice-reducible to a (u_i) -tree which is isomorphic to the full binary tree. Then reversing the splice operations behind this reduction, we get a sequence of node splitting operations that transform an isomorphic (u_i) -copy of the full binary tree into T . Since this (u_i) -copy of the full binary tree has a full labeling, by making these labels persistent during the series of splitting operations that lead to T , we get a full labelling of T . \square

The work in [BLP16] shows that if (u_i) is an increasing computable sequence, then any tree of measure more than $\sum_i 2^{i-u_i} < \mu(\mathcal{P})$ has a full labelling. Moreover, such a labelling has a Π_1^0 approximation, given any Π_1^0 approximation of \mathcal{P} .

References

- [BDN11] George Barmpalias, Rod Downey, and Keng Meng Ng. Jump inversions inside effectively closed sets and applications to randomness. *J. Symbolic Logic*, 76(2):491–518, 2011.

⁵A similar remark can be made with respect to the Gács coding, only that instead of binary trees we need to consider a homogeneous trees, in the sense that for each level, every node of that level has the same number of successors.

- [Ben88] Charles H. Bennett. Logical depth and physical complexity. In R. Herken, editor, *The universal Turing machine, a half century survey*, pages 227–257. Oxford U.P., 1988.
- [BGK⁺15] Laurent Bienvenu, Noam Greenberg, Antonín Kučera, André Nies, and Dan Turetsky. Coherent randomness tests and computing the K -trivial sets. *Journal of the European Mathematical Society*, 2015.
- [BLN10] George Barmpalias, Andrew E. M. Lewis, and Keng Meng Ng. The importance of Π_1^0 classes in effective randomness. *J. Symbolic Logic*, 75(1):387–400, 2010.
- [BLP16] George Barmpalias and Andy Lewis-Pye. Optimal redundancy in computations from random oracles. Preprint, ArXiv:1606.07910, 2016.
- [BLPT16] George Barmpalias, Andrew Lewis-Pye, and Jason Teutsch. Lower bounds on the redundancy in computations from random oracles via betting strategies with restricted wagers. *Inform. and Comput.*, 251:287–300, 2016.
- [DM06] Rod G. Downey and Joseph S. Miller. A basis theorem for Π_1^0 classes of positive measure and jump inversion for random reals. *Proc. Amer. Math. Soc.*, 134(1):283–288 (electronic), 2006.
- [DM15] Adam Day and Joseph S. Miller. Density, forcing, and the covering problem. *Mathematical Research Letters*, 22:719–727,, 2015.
- [Dot06] David Doty. Every sequence is decompressible from a random one. In *Logical Approaches to Computational Barriers, Second Conference on Computability in Europe, CiE 2006, Swansea, UK, June 30-July 5, 2006, Proceedings*, pages 153–162, 2006.
- [Gác86] Péter Gács. Every sequence is reducible to a random one. *Inform. and Control*, 70(2-3):186–192, 1986.
- [Kha15] Mushfeq Khan. Lebesgue density and Π_1^0 -classes. *Journal of Symbolic Logic*, 2015. In press.
- [Kuč85] Antonín Kučera. Measure, Π_1^0 -classes and complete extensions of PA. In *Recursion theory week (Oberwolfach, 1984)*, volume 1141 of *Lecture Notes in Math.*, pages 245–259. Springer, Berlin, 1985.
- [Kuč89] Antonin Kučera. On the use of diagonally nonrecursive functions. In *Logic Colloquium '87 (Granada, 1987)*, volume 129 of *Stud. Logic Found. Math.*, pages 219–239. North-Holland, Amsterdam, 1989.
- [MM04] Wolfgang Merkle and Nenad Mihailović. On the construction of effectively random sets. *J. Symb. Log.*, 69(3):862–878, 2004.
- [MNZ15] Kenshi Miyabe, André Nies, and Jing Zhang. Using almost-everywhere theorems from analysis to study randomness. Preprint., 2015.
- [Nie09] André Nies. *Computability and Randomness*. Oxford University Press, 2009.